

Amendments to the Claims

1 Claim 1 (currently amended): A computer program product for efficiently generating pseudo-
2 random bits, the computer program product embodied on one or more computer readable media
3 and comprising:

4 computer-readable program code means for providing an input value;

5 computer-readable program code means for generating an output sequence of pseudo-
6 random bits using the provided input value as an exponent of input to a 1-way function
7 comprising modular exponentiation modulo a safe prime number, wherein a length in bits, C, of
8 the input value is substantially shorter than a length in bits, N, of the generated output sequence
9 and a base of the modular exponentiation is a fixed generator value; and

10 computer-readable program code means for using C selected bits of the generated output
11 sequence as the provided input value for a next iteration of the computer-readable program code
12 means for generating while using all N - C remaining bits of the generated output sequence as
13 pseudo-random output bits, until a desired number of pseudo-random output bits have been
14 generated.

1 Claim 2 (original): The computer program product according to Claim 1, wherein the 1-way
2 function is based upon an assumption known as "the discrete logarithm with short exponent"
3 assumption.

Claims 3 - 5 (canceled)

Serial No. 09/753,727

-4-

RSW920000091US1

1 Claim 6 (currently amended): The computer program product according to Claim [[4]] 1,
2 wherein the length of the input value is 160 bits and a length of the safe prime number is 1024
3 bits.

1 Claim 7 (original): The computer program product according to Claim 1, wherein the length of
2 the input value is at least 160 bits and the length of the generated output sequence is at least 1024
3 bits.

Claim 8 (canceled)

1 Claim 9 (previously presented): The computer program product according to Claim 1, wherein
2 the N - C remaining bits are concatenated to pseudo-random output bits previously generated by
3 the computer-readable program code means for generating.

1 Claim 10 (previously presented): The computer program product according to Claim 1, wherein
2 the N - C remaining bits are selected from the N bits of the generated output sequence as a
3 contiguous group of bits.

1 Claim 11 (previously presented): The computer program product according to Claim 1, wherein
2 the N - C remaining bits are selected from the N bits of the generated output sequence as a non-
3 contiguous group of bits.

Serial No. 09/753,727

-5-

RSW920000091US1

1 Claim 12 (previously presented): The computer program product according to Claim 1, further
2 comprising computer-readable program code means for using the desired number of generated
3 pseudo-random bits as input to an encryption operation.

1 Claim 13 (currently amended): A system for efficiently generating pseudo-random bits in a
2 computing environment, comprising:

3 means for providing an input value;

4 means for generating an output sequence of pseudo-random bits using the provided input
5 value as an exponent of input to a 1-way function comprising modular exponentiation modulo a
6 safe prime number, wherein a length in bits, C, of the input value is substantially shorter than a
7 length in bits, N, of the generated output sequence and a base of the modular exponentiation is a
8 fixed generator value; and

9 means for using C selected bits of the generated output sequence as the provided input
10 value for a next iteration of the means for generating while using all N - C remaining bits of the
11 generated output sequence as pseudo-random output bits, until a desired number of pseudo-
12 random output bits have been generated.

1 Claim 14 (original): The system according to Claim 13, wherein the 1-way function is based
2 upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 15 - 17 (canceled)

Serial No. 09/753,727

-6-

RSW92000091US1

1 Claim 18 (currently amended): The system according to Claim ~~[[16]]~~ 13, wherein the length of
2 the input value is 160 bits and a length of the safe prime number is 1024 bits.

1 Claim 19 (original): The system according to Claim 13, wherein the length of the input value is
2 at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 20 (canceled)

1 Claim 21 (previously presented): The system according to Claim 13, wherein the N - C
2 remaining bits are concatenated to pseudo-random output bits previously generated by the means
3 for generating.

1 Claim 22 (previously presented): The system according to Claim 13, wherein the N - C
2 remaining bits are selected from the N bits of the generated output sequence as a contiguous
3 group of bits.

1 Claim 23 (previously presented): The system according to Claim 13, wherein the N - C
2 remaining bits are selected from the N bits of the generated output sequence as a non-contiguous
3 group of bits.

1 Claim 24 (previously presented): The system according to Claim 13, further comprising means
2 for using the desired number of generated pseudo-random output bits as input to an encryption

Serial No. 09/753,727

-7-

RSW920000091US1

operation.

Claim 25 (currently amended): A method for efficiently generating pseudo-random bits, comprising the steps of:

- providing an input value;
- generating an output sequence of pseudo-random bits using the provided input value as an exponent of input to a 1-way function comprising modular exponentiation modulo a safe prime number, wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and a base of the modular exponentiation is a fixed generator value; and
- using C selected bits of the generated output sequence as the provided input value for a next iteration of the generating step while using all N - C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.

Claim 26 (original): The method according to Claim 25, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 27 - 29 (canceled)

Claim 30 (currently amended): The method according to Claim ~~[[28]]~~ 25, wherein the length of the input value is at least 160 bits and a length of the safe prime number is at least 1024 bits.

Serial No. 09/753,727

-8-

RSW920000091US1

1 Claim 31 (original): The method according to Claim 25, wherein the length of the input value is
2 160 bits and the length of the generated output sequence is 1024 bits.

1 Claim 32 (original): The method according to Claim 25, wherein the length of the input value is
2 at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 33 (canceled)

1 Claim 34 (previously presented): The method according to Claim 25, wherein the N - C
2 remaining bits are concatenated to pseudo-random output bits previously generated by the
3 generating step.

1 Claim 35 (previously presented): The method according to Claim 25, wherein the N - C
2 remaining bits are selected from the N bits of the generated output sequence as a contiguous
3 group of bits.

1 Claim 36 (previously presented): The method according to Claim 25, wherein the N - C
2 remaining bits are selected from the N bits of the generated output sequence as a non-contiguous
3 group of bits.

1 Claim 37 (previously presented): The method according to Claim 25, further comprising the step

Serial No. 09/753,727,

-9-

RSW920000091US1

2 of using the desired number of generated pseudo-random output bits as input to an encryption
3 operation.

Claim 38 (canceled)

1 Claim 39 (currently amended): An encryption system, comprising:

2 means for providing an input value;

3 means for generating an output sequence of pseudo-random bits using the provided input
4 value as an exponent of input to a 1-way function comprising modular exponentiation modulo a
5 safe prime number, wherein a length in bits, C, of the input value is substantially shorter than a
6 length in bits, N, of the generated output sequence and a base of the modular exponentiation is a
7 fixed generator value;

8 means for using C selected bits of the generated output sequence as the provided input
9 value for a next iteration of the means for generating while using all N - C remaining bits of the
10 generated output sequence as pseudo-random output bits, until a desired number of pseudo-
11 random output bits have been generated; and

12 means for using the desired number of generated pseudo-random bits as input to an
13 encryption operation.

1 Claim 40 (original): The encryption system according to Claim 39, wherein the 1-way function
2 is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Serial No. 09/753,727

-10-

RSW920000091US1

Claims 41 - 43 (canceled)

1 **Claim 44 (currently amended):** The encryption system according to Claim ~~[[42]]~~ 39, wherein the
2 length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

1 **Claim 45 (original):** The encryption system according to Claim 39, wherein the length of the
2 input value is 160 bits and the length of the generated output sequence is 1024 bits.

Claim 46 (canceled)

1 **Claim 47 (currently amended):** The encryption system according to Claim ~~[[46]]~~ 39, wherein the
2 N - C remaining bits are concatenated to pseudo-random output bits previously generated by the
3 means for generating.